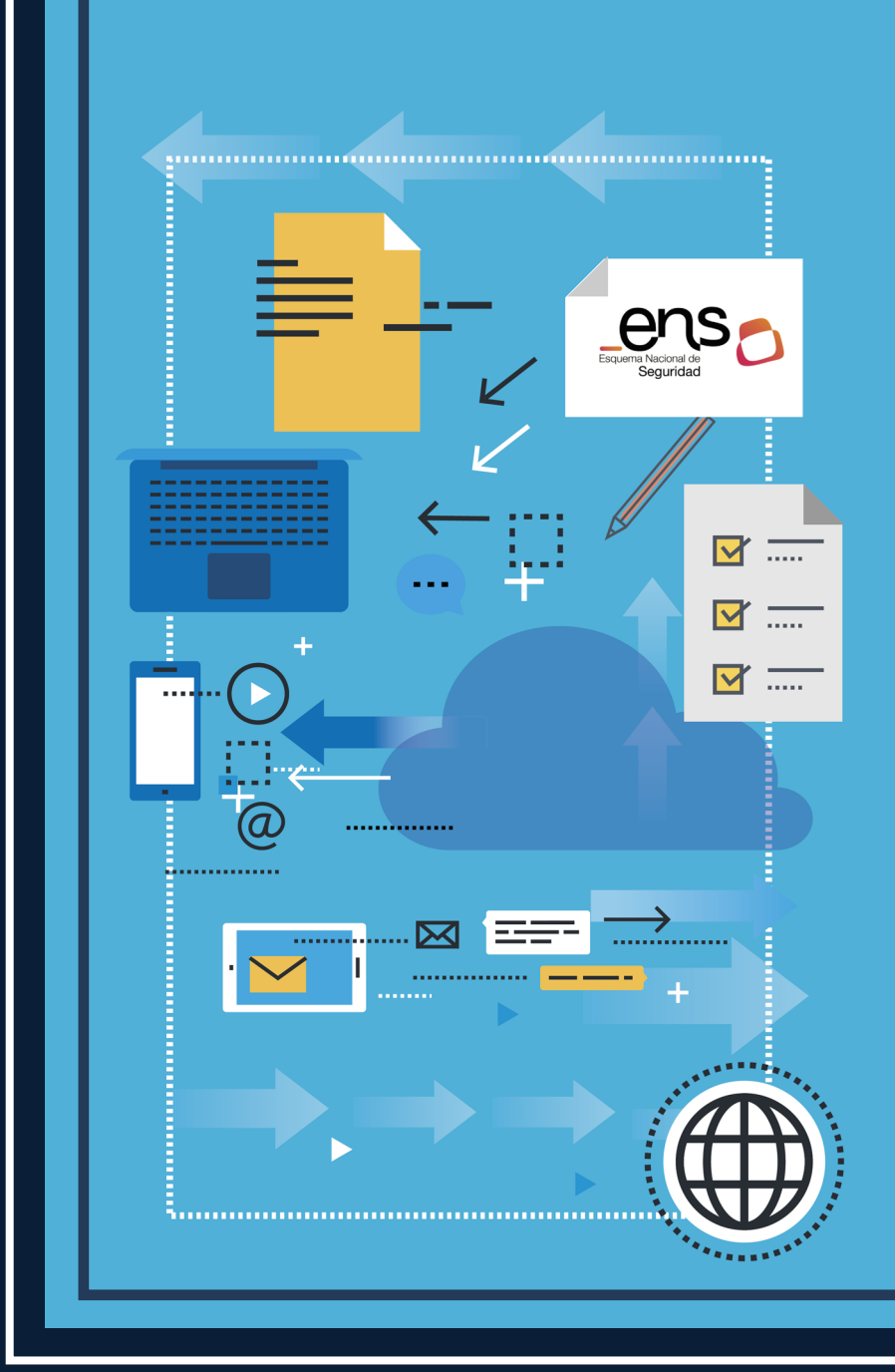
CCN-CERT

BP/14



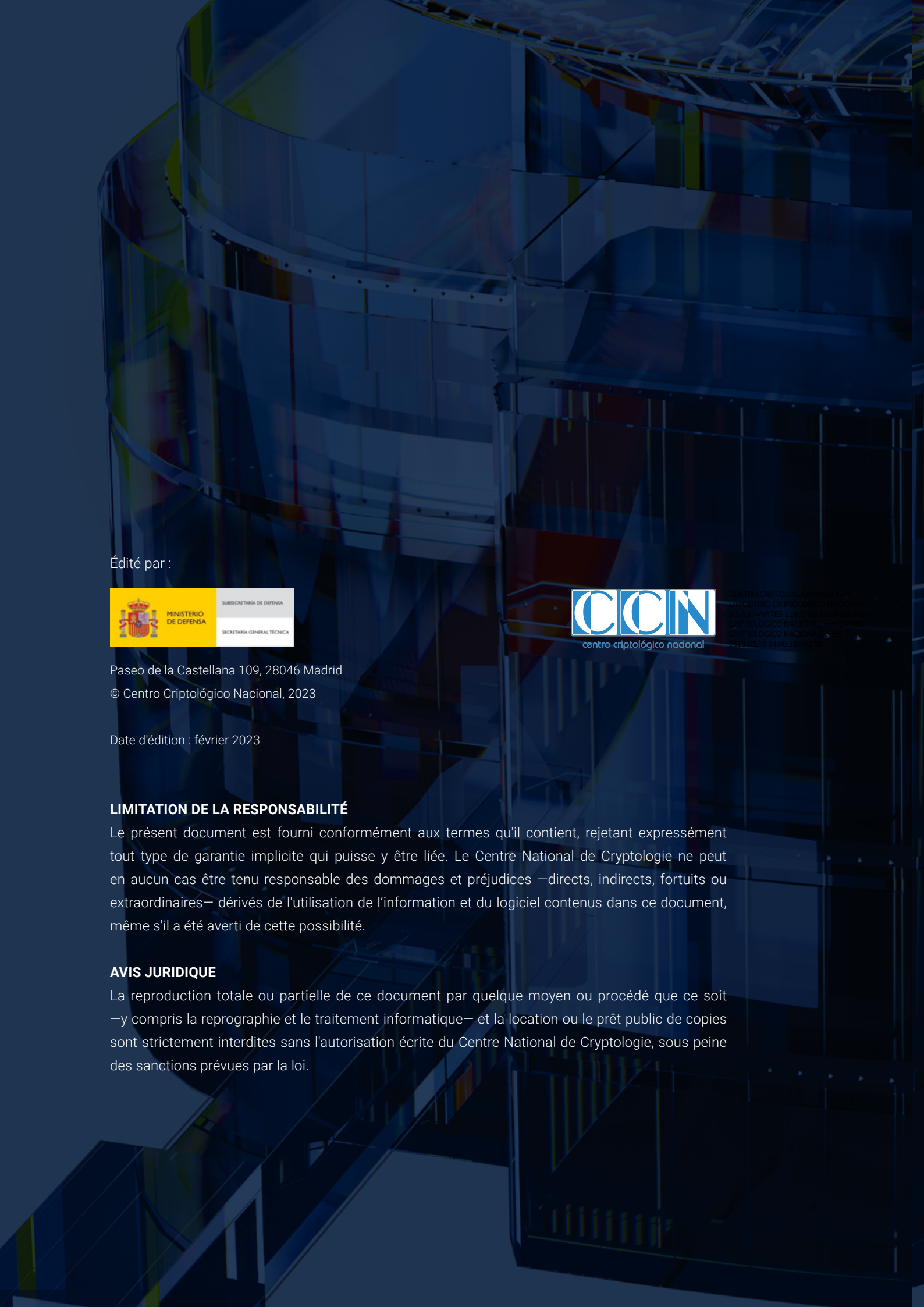
Déclaration d'Applicabilité dans l'ENS

RAPPORT DE BONNES PRATIQUES

FÉVRIER **2023**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional



Édité par :

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
centro criptológico nacional

Paseo de la Castellana 109, 28046 Madrid

Date d'édition : février 2023

LIMITATION DE LA RESPONSABILITÉ

Le présent document est fourni conformément aux termes qu'il contient, rejetant expressément tout type de garantie implicite qui puisse y être liée. Le Centre National de Cryptologie ne peut en aucun cas être tenu responsable des dommages et préjudices —directs, indirects, fortuits ou extraordinaires— dérivés de l'utilisation de l'information et du logiciel contenus dans ce document, même s'il a été averti de cette possibilité.

AVIS JURIDIQUE

Index

1. À propos du CCN-CERT, le CERT gouvernemental espagnol

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre National de Cryptologie, CCN, rattaché au Centre National de Renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT gouvernemental espagnol** et ses fonctions sont définies dans la Loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma national de sécurité (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en tant que centre national d'alerte et de réponse qui coopère et aide à réagir rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau national des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

L'objectif étant de disposer d'un cyberespace plus sécurisé et fiable, par la préservation de l'information classifiée (comme le stipule l'art. 4. F de la Loi 11/2002) et des informations sensibles, la défense du patrimoine technologique espagnol, la formation du personnel spécialisé, l'application de politiques et de procédures de sécurité, ainsi que l'utilisation et le développement des technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la Loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est responsable de la gestion des cyberincidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyberincidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre National de Cryptologie

2. Introduction

La Déclaration d'Applicabilité, dans le cadre de l'ENS, est un document qui établit la liste de mesures de sécurité applicables à un système d'information, en fonction de sa catégorie, et décrites dans l'Annexe II du Décret Royal 311/2022 du 3 mai.

Comme indiqué à l'article 38.3 de l'ENS, les mesures de sécurité énoncées dans l'Annexe II pourront être remplacées par d'autres mesures compensatoires, à condition qu'il soit prouvé —au moyen de documents— que celles-ci protègent les actifs autant sinon plus que les autres et que les principes de base et les exigences minimales énoncés dans le Décret Royal 311/2022, Chapitres II et III, soient respectés.

De même, comme le souligne le guide CCN-STIC-808 intitulé "Vérification de la conformité aux mesures de l'ENS", des mesures de vigilance complémentaires peuvent être prises afin de compléter et équilibrer les conditions requises pour pouvoir mettre en oeuvre une mesure de sécurité précise, qu'il s'agisse d'une mesure basique ou de renforcement, si l'organisme juge qu'elles sont insuffisantes pour pouvoir atteindre la conformité à l'ENS. Elles peuvent également compléter une mesure compensatoire qui ne parvient pas à égaler ou à réduire le niveau de risque de la mesure initiale. Parfois, ces mesures sont transitoires (limitées dans le temps) jusqu'à ce que la mise en œuvre de la mesure soit pleinement efficace.

.

La Déclaration d'Applicabilité, dans le cadre de l'ENS, est un document qui établit la liste de mesures de sécurité applicables à un système d'information, en fonction de sa catégorie

En tant que partie intégrante de la Déclaration d'Applicabilité, il sera nécessaire de rendre compte de la corrélation entre les mesures compensatoires implémentées et les mesures compensatoires figurant à l'Annexe II. Il faudra aussi spécifier toute mesure de vigilance supplémentaire qui soit éventuellement requise, laquelle fera l'objet de l'approbation officielle du responsable de sécurité.

Le document formalisé sera essentiel pour préparer un plan de mise en conformité et, ensuite, pour mettre en place les mesures prévues. Il pourra être analysé par l'autorité de certification et utilisé comme document d'appui lors de l'audit pour la mise en conformité à l'ENS. À cette fin, il est important de définir lesquelles des 73 mesures de sécurité énumérées dans l'ENS sont applicables au système d'information ou au sein de l'organisation. Pour chaque mesure, il est important de rédiger une description assez courte sur la méthode de mise en œuvre, mais aussi les documents de références prouvant leur insertion. Le cas échéant, il faudra justifier les raisons de leur exclusion.

Le document formalisé sera essentiel pour préparer un plan de mise en conformité et, ensuite, pour mettre en place les mesures prévues

3. Définition de la Déclaration d'Applicabilité

Il est indispensable de catégoriser les mesures et de suivre les indications spécifiées dans l'Annexe I de l'ENS de manière à mettre en conformité le système d'information avec les dispositions de l'ENS et pouvoir déterminer quelles sont les mesures à appliquer.

Le processus de catégorisation a pour but d'attribuer une catégorie BASIQUE, MOYENNE ou ÉLEVÉE aux systèmes d'information. La catégorie d'un système d'information —en termes de sécurité— vise à établir un équilibre entre l'importance de l'information qu'il traite, les services qu'il fournit et les efforts de sécurité requis, tout comme les risques auxquels il est exposé, selon les critères du principe de proportionnalité.

Autrement dit, les mesures de sécurité à appliquer au système d'information, figurant dans la Déclaration d'Applicabilité, découlent principalement de la catégorisation du système, ce qui donne lieu à un ensemble de valeurs par mesure (conditions basiques et renforcements obligatoires). Cependant, il existe aussi des cas où ces mesures peuvent être sélectionnées quand les actions d'atténuation de risques sont jugées inacceptables (renforcements optionnels ou renforcements obligatoires pour une catégorie plus élevée).

La catégorie est fixée en fonction de l'évaluation de l'impact d'un incident sur la sécurité de l'information ou des services et de son atteinte aux dimensions de la sécurité : **disponibilité [D], authenticité [A], intégrité [I], confidentialité [C]** ou **traçabilité [T]**, selon la procédure établie à l'Annexe I du Décret Royal 311/2022.

Le processus de catégorisation a pour but d'attribuer une catégorie BASIQUE, MOYENNE ou ÉLEVÉE aux systèmes d'information

3.1. Catégorisation

La **catégorie d'un système** (BASIQUE, MOYENNE ou ÉLEVÉE) s'établit en fonction de l'évaluation de l'impact qu'un incident de sécurité de ce système d'information pourrait avoir sur l'organisation, en modifiant sa capacité organisationnelle à :

a) Atteindre ses objectifs.
b) Protéger les actifs qu'elle a à sa charge, y compris l'information.
c) Accomplir ses obligations de service quotidiennes.
d) Respecter la loi en vigueur.
e) Respecter les droits des personnes.

L'évaluation de cet impact se fait non seulement pour chaque dimension, mais aussi de manière individuelle pour chaque actif du système d'information, d'où la nécessité de disposer d'un inventaire actualisé de ces actifs.

En premier lieu, il est recommandé d'évaluer les actifs essentiels (information et services) car ceux-ci exigent un examen plus exhaustif au moment de fixer les niveaux de sécurité (selon les dimensions) qui serviront de base à l'établissement de la catégorie du système. Les actifs essentiels sont tous ceux qui concentrent la valeur du système —du point de vue de la sécurité— et qui constituent l'essence et la raison d'être du système. Le reste des actifs viendront renforcer les actifs essentiels mentionnés et leurs valeurs seront identiques grâce au processus d'instanciation et à leur relation de dépendance.

Bien qu'il s'agisse d'un service à fournir ou d'une information, il est conseillé de se concentrer sur l'évaluation des dimensions spécifiques. Par exemple, il est opportun d'évaluer les dimensions de **confidentialité** et **d'intégrité (C, I)** quand il s'agit d'actifs informationnels, alors que la dimension de **disponibilité (D)** est souvent associée aux actifs de service.

Les deux (2) autres dimensions, telles que l'**authenticité (A)** et la **traçabilité (T)**, sont indistinctement associées aux services ou à l'information, selon ce qui convient le mieux à l'organisation. L'important c'est qu'elles soient prises en compte, d'une manière ou d'une autre, au cas où elles puissent être applicables..

La catégorie d'un système s'établit en fonction de l'évaluation de l'impact qu'un incident de sécurité de ce système d'information pourrait avoir sur l'organisation

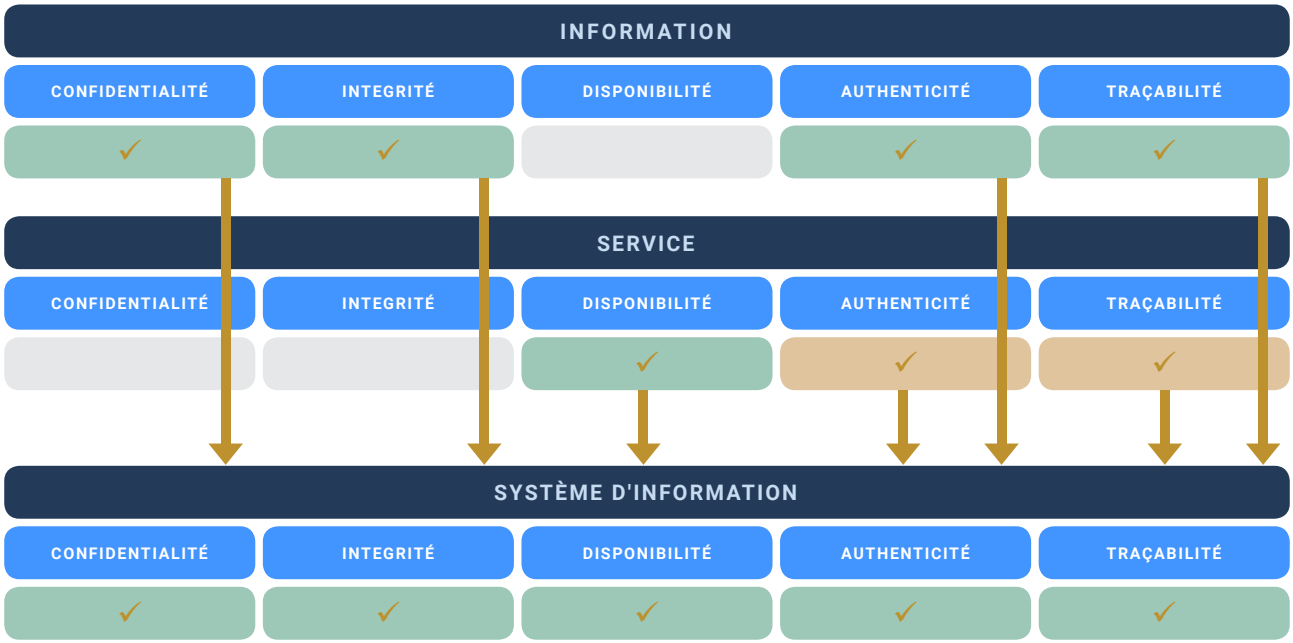


Figure 1. Évaluation des dimensions en fonction de l'actif.

3.1.1 Détermination du niveau de sécurité pour chaque dimension

L'ENS établit trois (3) **niveaux de sécurité** pour les différentes dimensions : Faible [F], Moyen [M] et Élevé [É].

Le niveau de sécurité (pour chaque dimension) sera obtenu à partir de l'évaluation de l'impact réel que les risques suivants pourraient avoir sur l'entité :

- **Disposition légale :** existence d'une disposition légale ou administrative qui conditionne le niveau de la dimension.
- **Préjudice direct :** existence d'un préjudice direct encouru par le citoyen.
- **Non-respect d'une norme :** entraîne le non-respect d'une norme (juridique, réglementaire, contractuelle ou interne).
- **Pertes économiques :** entraîne des pertes économiques pour l'entité.
- **Réputation :** porte atteinte à la réputation de l'entité.
- **Protestations :** prévoit la possibilité que ça puisse déboucher sur des protestations.
- **Criminalité :** rendrait plus facile la commission de délits et plus difficile les travaux d'enquête.

TABLEAU 1. CRITÈRES COMMUNS APPLICABLES À TOUTES LES DIMENSIONS DES TYPES D'INFORMATION ET DE SERVICES

CRITICITÉ		NON RATTACHÉ	FAIBLE	MOYEN	ÉLEVÉ
Disposition légale ou administrative		Aucune disposition légale ne conditionne son niveau.	Par disposition légale ou administrative : loi, décret, arrêté, règlement, ...	Par disposition légale ou administrative : loi, décret, arrêté, règlement, ...	Par disposition légale ou administrative : loi, décret, arrêté, règlement, ...
Préjudice direct au citoyen		Ne représente aucun préjudice direct pour le citoyen.	Représente un préjudice mineur pour le citoyen.	Représente un préjudice important pour le citoyen. Réparable.	Représente un grave préjudice pour le citoyen.
Non-respect d'une norme	**Juridique**	N'entraîne pas le non-respect d'une norme juridique.	Non-conformité formelle mineure à une norme juridique. Réparable.	Violation substantielle ou formelle d'une norme juridique. Irréparable.	Non-conformité critique à une norme juridique.
	Réglemen-taire	N'entraîne pas le non-respect des normes fixées par un organisme de réglementation.	Entraîne le non-respect des normes fixées par un organisme de réglementation.	Entraîne une sanction importante imposée par un organisme de réglementation.	Entraîne une sanction sévère imposée par un organisme de réglementation et/ou la perte de l'autorisation d'exercer.
	Contractuelle	N'entraîne pas le non-respect d'une obligation contractuelle.	Violation mineure d'une obligation contractuelle.	Violation substantielle ou formelle d'une obligation contractuelle.	Violation grave d'une obligation contractuelle.
	Interne	N'entraîne pas le non-respect des normes internes.	Violation mineure d'une norme interne.	Violation substantielle ou formelle d'une norme interne.	Violation grave d'une norme interne.
Pertes économiques		Ne provoque pas de pertes économiques.	Pertes économiques importantes (inférieures à 4 % du budget annuel de l'organisation).	Pertes économiques importantes (égales ou supérieures à 4 % et inférieures à 10 % du budget annuel de l'organisation).	Pertes économiques ou troubles financiers importants (égales ou supérieures à 10 % du budget annuel de l'organisation).
Réputation		Ne porte pas atteinte à la réputation.	Préjudice réputationnel notoire auprès des citoyens ou d'autres organisations.	Préjudice réputationnel important auprès des citoyens ou d'autres organisations.	Préjudice réputationnel grave auprès des citoyens et d'autres organisations.
Protestations		Il n'est pas prévu que ça puisse déboucher sur des protestations.	Nombreuses actions de protestation individuelles.	Protestations publiques (trouble à l'ordre public).	Protestations de masse (trouble à l'ordre public grave).
Délits		Ne faciliterait pas la commission de délits et n'entraverait pas les travaux d'enquête.	Pourrait favoriser la commission de délits.	Pourrait favoriser notablement la commission de délits ou rendre les travaux d'enquête plus difficiles.	Pourrait inciter à la commission de délits, constituer une infraction en soi ou entraver énormément les travaux d'enquête.

3.1.2 Détermination de la catégorie

L'ENS établit trois (3) **catégories de sécurité** pour les systèmes d'information : BASIQUE, MOYENNE et ÉLEVÉE :

- Un système d'information est de **catégorie ÉLEVÉE** si l'une de ses dimensions atteint le Niveau Élevé.
- Un système d'information est de **catégorie MOYENNE** si l'une de ses dimensions atteint le Niveau Moyen et qu'aucune n'atteint un niveau supérieur.
- Un système d'information est de **catégorie BASIQUE** si l'une de ses dimensions atteint le Niveau Faible et qu'aucune n'atteint un niveau supérieur.

La catégorisation d'un système n'entraîne aucune modification sur le niveau des dimensions qui n'ont pas eu d'influence sur la détermination de la catégorie de ce système. Toutefois, il convient de noter que l'attribution d'une catégorie au système nécessite de fixer le niveau de maturité des mesures à appliquer.

La catégorisation d'un système n'entraîne aucune modification sur le niveau des dimensions qui n'ont pas eu d'influence sur la détermination de la catégorie de ce système

3.2. Détermination des mesures d'application

Afin de se conformer aux principes de base et aux exigences minimales définis dans l'ENS, il convient d'appliquer un ensemble de mesures de sécurité qui soient nécessairement proportionnelles aux dimensions pertinentes du système à protéger et à sa catégorie.

L'Annexe II du Décret Royal 311/2022 établit la correspondance entre les niveaux de sécurité requis pour chaque dimension et les mesures de sécurité applicables.

Plus précisément, pour chaque mesure de sécurité, il est indiqué :

- Si son application est déterminée par la catégorie du système ou par le niveau de sécurité attribué à une ou plusieurs dimensions.
- - Si elle est applicable ou non pour un niveau de sécurité précis. Si l'application de la mesure n'est pas nécessaire pour atteindre les exigences de l'ENS, la valeur **"n.a."** (non applicable) figure dans le tableau de l'Annexe II.

En revanche, si son application est nécessaire, l'une des valeurs suivantes apparaîtra :

- **"applicable" :** indique qu'une mesure de sécurité doit être appliquée nécessairement, à un certain niveau, à une ou plusieurs dimensions afin de couvrir les **exigences de base**.
- **"+Rn"** : où "n" peut adopter une valeur comprise entre le "1" et le "9"; indique que ce **renforcement obligatoire** doit être appliqué, à un certain niveau, à une ou plusieurs dimensions.

À un certain niveau, il est possible d'appliquer simultanément plusieurs renforcements obligatoires à une ou plusieurs dimensions, comme par exemple: "R1 + R2 + R5". De même, il peut être nécessaire de sélectionner parmi un sous-ensemble de renforcements obligatoires un en particulier, comme par exemple: "R1 ou R2 ou R3". Les deux cas peuvent être combinés, comme par exemple : "[R1 ou R2 ou R3] + R9".

Il convient d'appliquer un ensemble de mesures de sécurité qui soient nécessairement proportionnelles aux dimensions pertinentes du système à protéger et à sa catégorie

Voici quelques exemples de ce qui a été décrit ci-dessus :

a • La mesure [org.1] s'applique aux systèmes de toutes les catégories. Le niveau d'exigence de la mesure ne varie pas en fonction de la catégorie associée au système; seules les **exigences de base** s'appliquent à toutes les catégories.

Affectées	BASIQUE	MOYENNE	ÉLEVÉE	Mesure de sécurité	
Catégorie	applicable	applicable	applicable	[org.1]	Politique de sécurité

b • La mesure [mp.if.6] s'applique aux systèmes dont le niveau de sécurité associé à la dimension de *Disponibilité* est Moyen ou Élevé. Le niveau d'exigence de la mesure ne varie pas selon qu'il s'agisse du Niveau Moyen ou du Niveau Élevé. Dans les deux cas, seules les **exigences de base** s'appliquent.

Affectées	FAIBLE	MOYENNE	ÉLEVÉE	Mesure de sécurité	
D	n.a.	applicable	applicable	[mp.if.6]	Protection contre les inondations

c • La mesure [mp.si.2] s'applique aux systèmes dont le niveau de sécurité associé aux dimensions de *Confidentialité* ou d'*Intégrité* est Moyen ou Élevé. Le niveau d'exigence de la mesure change si l'un des niveaux est Moyen ou Élevé. Les **exigences de base** sont les mêmes pour les Niveaux Moyen et Élevé, tandis que les renforcements optionnels ne s'appliquent qu'au Niveau Élevé dans ces deux (2) dimensions.

Affectées	FAIBLE	MOYENNE	ÉLEVÉE	Mesure de sécurité	
C I	n.a.	applicable	+R1 +R2	[mp.si.2]	Cryptographie

d • La mesure [mp.com.4] ne s'applique pas à la catégorie BASIQUE. Le niveau d'exigence de la mesure sera différent selon qu'il s'agisse d'une catégorie MOYENNE ou ÉLEVÉE. Les **exigences de base** s'appliquent aux deux catégories; pour la catégorie MOYENNE, il faudra faire le choix entre les **renforcements obligatoires** R1, R2 ou R3 ; tandis que pour la catégorie ÉLEVÉE, le **renforcement obligatoire R4** doit toujours s'appliquer, ainsi que l'option choisie entre R2 et R3.

Affectées	BASIQUE	MOYENNE	ÉLEVÉE	Mesure de sécurité	
Catégorie	n.a.	+ [R1 ou R2 o R3]	+ [R2 ou R3] + R4	[mp.com.4]	Séparation des flux d'information en réseau

4. Exemple

4.1. Catégorisation

Prenons l'exemple simple d'une entité locale qui, en raison de sa nature publique, relève du champ d'application de l'ENS.

Nous suivons les étapes suivantes :

1 · **Inventaire des actifs**
Au lieu de réaliser un inventaire complet, nous nous concentrons sur les actifs qui s'avèrent essentiels pour le Système d'Information dans le cadre défini :

- Information liée au Registre Nominal des Habitants (PMH).
- Information liée au Registre.
- Service du Registre Nominal des Habitants (PMH).
- Service du Registre.

2 · **Évaluation des actifs**
Après avoir analysé l'impact potentiel d'un incident sur les actifs essentiels, les niveaux de sécurité affectés à chaque dimension sont les suivants :

ACTIFS INFORMATION	[D]	[I]	[C]	[A]	[T]
Information liée au Registre Nominal des Habitants	n.a.	[M]	[M]	[M]	[M]
Information liée au Registre	n.a.	[M]	[M]	[M]	[M]

ACTIFS SERVICES	[D]	[I]	[C]	[A]	[T]
Service du Registre Nominal des Habitants	[M]	n.a.	n.a.	[F]	[F]
Service du Registre E/S	[M]	n.a.	n.a.	[F]	[F]

Les niveaux de sécurité en matière d'*Intégrité* et de *Confidentialité* n'ont pas été évalués pour les actifs "Service" (valeur fixée à "**n.a.**"), car ils sont une instanciation des niveaux attribués aux actifs "Information". De la même façon, le niveau de sécurité associé à la *Disponibilité* pour les actifs "Information" est déterminé selon le niveau associé aux services.

3 · Regroupement et instanciation

ACTIFS INFORMATION	[D]	[I]	[C]	[A]	[T]
Information liée au Registre Nominal des Habitants	[M]	[M]	[M]	[M]	[M]
Information liée au Registre	[M]	[M]	[M]	[M]	[M]
Niveau maximal de l'Information	[M]	[M]	[M]	[M]	[M]

ACTIFS SERVICES	[D]	[I]	[C]	[A]	[T]
Service du Registre Nominal des Habitants	[M]	[M]	[M]	[F]	[F]
Service du Registre	[M]	[M]	[M]	[F]	[F]
Niveau maximal des Services	[M]	[M]	[M]	[F]	[F]

VALEURS MAXIMALES DU SYSTÈME	[D]	[I]	[C]	[A]	[T]	VALEUR MAXIMALE
Information liée au Registre Nominal des Habitants	[M]	[M]	[M]	[M]	[M]	[M]
Information liée au Registre	[M]	[M]	[M]	[M]	[M]	[M]

Les niveaux du système sont les suivants : [D] = M, [I] = M, [C] = M, [A] = M et [T] = M.

4 · Détermination de la catégorie

L'analyse des niveaux attribués permet de déterminer que la catégorie du système d'information est MOYENNE.

Il convient de noter que la détermination de la catégorie du système d'information ne modifie pas le niveau de sécurité des dimensions individuelles, ces dimensions étant pertinentes pour déterminer l'applicabilité de certaines mesures de l'Annexe II du Décret Royal 311/2022. Cette casuistique sera exemplifiée dans les sections suivantes de ce guide.

VALEURS MAXIMALES DU SYSTÈME	[D]	[I]	[C]	[A]	[T]	VALEUR MAXIMALE
Information liée au Registre Nominal des Habitants	[M]	[M]	[M]	[M]	[M]	[M]
Valeurs des Services	[M]	[M]	[M]	[B]	[B]	[M]
Catégorie du système						[M]

4.2. Détermination de la Déclaration d'Applicabilité

Exemple 1 : Système d'information possédant les niveaux suivants :

SYSTÈME 1		
NIVEAUX DES DIMENSIONS	CONFIDENTIALITÉ (C)	**Élevé**
	INTÉGRITÉ (I)	**Élevé**
	DISPONIBILITÉ (D)	**Moyen**
	AUTHENTICITÉ (A)	**Élevé**
	TRAÇABILITÉ (T)	**Faible**

Sa catégorie correspond au niveau le plus élevé associé à l'une des dimensions. Par conséquent, la **catégorie de ce système est ÉLEVÉE: [D(M), I(É), C(É), A(É), T(F)]**.

Les mesures à appliquer sont celles requises pour le niveau Élevé, sauf celles qui ne s'appliquent qu'à la *Traçabilité* (Niveau Moyen ou Élevé) et à la *Disponibilité* (Niveau Élevé).

En d'autres termes, en raison de la *Traçabilité* de Niveau Faible, la mesure [mp.info.4], signalée comme "NON APPLICABLE", ne sera pas applicable. D'autre part, en raison de la *Disponibilité* de Niveau Moyen, les mesures [op.cont.2], [op.cont.3] et [op.cont.4] ne seront pas applicables. Cependant, seul l'**exigence de base** s'applique dans le cas de [mp.s.4] et seul le **renforcement obligatoire** R1 s'applique dans le cas de [mp.info.6].

Les mesures à appliquer sont celles requises pour le niveau Élevé, sauf celles qui ne s'appliquent qu'à la *Traçabilité* (Niveau Moyen ou Élevé) et à la *Disponibilité* (Niveau Élevé)

4. Exemple

CODE	DESCRIPTION	DIMENSIONS	CATÉGORIE DU SYSTÈME
ORG	**CADRE ORGANISATIONNEL**		
org.1	Politique de sécurité	D I C A T	applicable
org.2	Règlement de sécurité	D I C A T	applicable
org.3	Procédures de sécurité	D I C A T	applicable
org.4	Processus d'autorisation	D I C A T	applicable
OP	**CADRE OPÉRATIONNEL**		
op.pl	**Planification**		
op.pl.1	Analyse de risques	D I C A T	+R2
op.pl.2	Architecture de sécurité	D I C A T	+R1 +R2 +R3
op.pl.3	Achat de nouveaux composants	D I C A T	applicable
op.pl.4	Dimensionnement/gestion de la capacité	D _ _ _ _	+R1
op.pl.5	Composants certifiés	D I C A T	applicable
op.acc	**Contrôle d'accès**		
op.acc.1	Identification	_ _ _ A T	+R1
op.acc.2	Conditions d'accès	_ I C A T	+R1
op.acc.3	Séparation des fonctions et des tâches	_ I C A T	+R1
op.acc.4	Processus de gestion des droits d'accès	_ I C A T	applicable
op.acc.5	Mécanisme d'authentification (utilisateurs externes)	_ I C A T	+ [R2 o R3 o R4] + R5
op.acc.6	Mécanisme d'authentification (utilisateurs de l'organisation)	_ I C A T	+ [R1 o R2 o R3 o R4] + R5 + R6 + R7 + R8 + R9
op.exp	**Exploitation**		
op.exp.1	Inventaire des actifs	D I C A T	applicable
op.exp.2	Paramètres de sécurité	D I C A T	applicable
op.exp.3	Gestion de la configuration de la sécurité	D I C A T	+R1 +R2 +R3
op.exp.4	Maintenance et mises à jour de sécurité	D I C A T	+R1 +R2
op.exp.5	Gestion du changement	D I C A T	+R1
op.exp.6	Protection contre les codes malveillants	D I C A T	+R1 +R2 +R3 +R4
op.exp.7	Gestion des incidents	D I C A T	+R1 +R2 +R3
op.exp.8	Enregistrement de l'activité	_ _ _ _ T	applicable
op.exp.9	Enregistrement des incidents (logs)	D I C A T	applicable
op.exp.10	Protection des clés cryptographiques	D I C A T	+R1
op.ext	**Ressources externes**		
op.ext.1	Accords contractuels et sur les niveaux de service	D I C A T	applicable
op.ext.2	Gestion quotidienne	D I C A T	applicable
op.ext.3	Sécurité de la chaîne d'approvisionnement	D I C A T	aplica
op.ext.4	Interconnexion des systèmes	D I C A T	+R1

CODE	DESCRIPTION	DIMENSIONS	CATÉGORIE DU SYSTÈME
ORG	CADRE ORGANISATIONNEL		
op.nub	Cloud Services		
op.nub.1	Protection des services cloud	D I C A T	+R1 +R2
op.cont	Continuité du service		
op.cont.1	Analyse d'impact	D _ _ _ _	applicable
op.cont.2	Plan de continuité	D _ _ _ _	n.a.
op.cont.3	Tests périodiques	D _ _ _ _	n.a.
op.cont.4	Médias alternatifs	D _ _ _ _	n.a.
op.mon	Surveillance du système		
op.mon.1	Détection des intrusions	D I C A T	+R1 +R2
op.mon.2	Système métrique	D I C A T	+R1 +R2
op.mon.3	Surveillance	D I C A T	+R1 +R2 +R3 +R4 +R5 +R6
MP	MESURES DE PROTECTION		
mp.if	Protection des installations et des infrastructures		
mp.if.1	Zones séparées et à accès contrôlé	D I C A T	applicable
mp.if.2	Identification des personnes	D I C A T	applicable
mp.if.3	État des lieux	D I C A T	applicable
mp.if.4	Énergie électrique	D _ _ _ _	+R1
mp.if.5	Protection contre les incendies	D _ _ _ _	applicable
mp.if.6	Protection contre les inondations	D _ _ _ _	applicable
mp.if.7	Contrôle de l'équipement	D I C A T	applicable
mp.per	Gestion du personnel		
mp.per.1	Caractérisation des postes de travail	D I C A T	applicable
mp.per.2	Devoirs et obligations	D I C A T	+R1
mp.per.3	Sensibilisation	D I C A T	applicable
mp.per.4	Formation	D I C A T	applicable
mp.eq	Protection des équipements		
mp.eq.1	Poste de travail épuré	D I C A T	+R1
mp.eq.2	Verrouillage du poste de travail	_ _ _ A _	+R1
mp.eq.3	Protection des appareils portables	D I C A T	+R1 +R2
mp.eq.4	Autres appareils connectés au réseau	_ _ C _ _	+R1
mp.com	Protection des communications		
mp.com.1	Périmètre sécurisé	D I C A T	applicable
mp.com.2	Protection de la confidentialité	_ _ C _ _	+R1 +R2 +R3
mp.com.3	Protection de l'intégrité et de l'authenticité	_ I _ A _	+R1 +R2 +R3 +R4
mp.com.4	Séparation des flux d'information dans le réseau	D I C A T	+[R2 o R3] +R4

4. Exemple

CODE	DESCRIPTION	DIMENSIONS	CATÉGORIE DU SYSTÈME
ORG	CADRE ORGANISATIONNEL		
mp.si	Protection des supports d'information		
mp.si.1	Marquage des supports	_ _ C _ _	applicable
mp.si.2	Cryptographie	_ I C _ _	+R1 +R2
mp.si.3	Dépôt	D I C A T	applicable
mp.si.4	Transport	D I C A T	applicable
mp.si.5	Effacement et destruction	_ _ C _ _	+R1
mp.sw	Protection des applications informatiques		
mp.sw.1	Développement d'applications	D I C A T	+R1 +R2 +R3 +R4
mp.sw.2	Acceptation et mise en service	D I C A T	+R1
mp.info	Protection de l'information		
mp.info.1	Données personnelles	D I C A T	applicable
mp.info.2	Qualification des informations	_ _ C _ _	applicable
mp.info.3	Signature électronique	_ I _ A _	+R1 +R2 +R3 +R4
mp.info.4	Horodatage (Timestamping)	_ _ _ _ T	n.a.
mp.info.5	Nettoyage des documents	_ _ C _ _	applicable
mp.info.6	Copies de sauvegarde	D _ _ _ _	+R1
mp.s	Protection des services		
mp.s.1	Protection du courrier électronique	D I C A T	applicable
mp.s.2	Protection des services et applications web	D I C A T	+R2 +R3
mp.s.3	Protection de la navigation web	D I C A T	+R1
mp.s.4	Protection contre le déni de service	D _ _ _ _	applicable

En résumé, sur les 73 mesures énumérées dans l'Annexe II du Décret Royal 311/2022, seules 69 sont applicables/exigées pour le système de l'exemple :

- 61 de Niveau d'exigence Élevé.
- 7 de Niveau d'exigence Moyen.
- 1 de Niveau d'exigence Faible.
- 4 non applicables.

5. Profil de conformité spécifique

Nous pouvons définir un Profil de Conformité Spécifique (PCS) comme l'ensemble des mesures de sécurité, comprises ou non dans l'Annexe II du RD 311/2022, qui —suite à l'étape obligée d'analyse de risques— sont applicables à une entité ou un secteur d'activité spécifique et pour une catégorie de sécurité spécifique.

Le CCN, dans l'exercice de ses compétences, valide et publie les profils de conformité spécifiques préalablement définis, ainsi que les schémas d'accréditation et de validation correspondants, conformément aux instructions techniques de sécurité et aux guides de sécurité approuvés en vertu de la deuxième disposition additionnelle de l'ENS.

Par conséquent, au moment de rédiger la Déclaration d'Applicabilité pour un système d'information donné, l'organisation devra considérer si ce système est éligible à un PCS et, le cas échéant, adapter la Déclaration d'Applicabilité à ce système.

Au moment de rédiger la Déclaration d'Applicabilité pour un système d'information donné, l'organisation devra considérer si ce système est éligible à un PCS et, le cas échéant, adapter la Déclaration d'Applicabilité à ce système

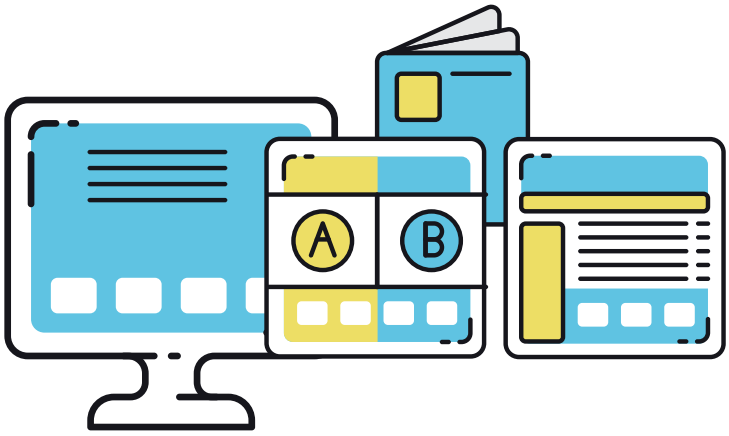
6. Recommandations

6.1. Concernant le format de la Déclaration d'Applicabilité

Il convient d'ajouter deux (2) colonnes supplémentaires afin que la Déclaration d'Applicabilité soit plus claire et utile : l'une faisant référence au **niveau d'implémentation** des mesures applicables (CCN-STIC-808) et l'autre justifiant leur **niveau de maturité** à travers une courte description sur la manière dont chaque mesure s'applique dans le Système d'Information de l'Organisation.

Cette description devra inclure une référence si une mesure de sécurité (qu'il s'agisse de la mesure en soi, de son renforcement basique ou d'un éventuel renforcement obligatoire) a été remplacée par une **mesure compensatoire**. Il en va de même si une mesure de sécurité particulière requiert des **mesures de contrôle supplémentaires**.

.



DÉCLARATION D'APPLICABILITÉ RD 311/2022									
DIMENSION	F	M	É	Mesure	Description	Con-forme	Niveau d'implé-mentation	Niveau de maturité	COMMENTAIRES SUR LA MANIÈRE D'APPLIQUER LES MESURES ET DOCUMENTS DE RÉFÉRENCES
CADRE ORGANISATIONNEL									
Catégorie	APPL	APPL	APPL	org.1	Politique de sécurité	OUI	G2	L3	On dispose du document "POL-001 Politique de sécurité ". Selon la gestion de versions, la dernière version de ce document corres-pond à la V1.1 du 24/10/2022. Ceci a été communiqué en interne via l'Intranet de l'organisation.
Catégorie	APPL	APPL	APPL	org.2	Règlement de sécurité	OUI	G2	L3	On dispose du document "NOR-001 Règlement d'Utilisation des systèmes" qui est spécifié dans la Politique de Sécurité. Le règlement d'utilisation des systèmes a été signé par les employés de l'organisation, leur signature figurant à la fin du dernier paragraphe.
Catégorie	APPL	APPL	=	org.3	Processus de sécurité	OUI	G2	L1	
Catégorie	APPL	APPL	APPL	org.4	Processus d'autorisation	OUI	G2	L1	
CADRE OPÉRATIONNEL									
				op.pl.	PLANIFICATION				
Catégorie	APPL	+R1	+R2	op.pl.1	Analyse de risques	OUI	G2	L2	
Catégorie	APPL	+R1	+R1 +R2 +R3	op.pl.2	Architecture de sécurité	OUI	G2	L2	
Catégorie	APPL	APPL	APPL	op.pl.3	Achat de nouveaux composants	OUI	G2	L2	
D	APPL	+R1	+R1	op.pl.4	Gestion des capacités	OUI	G0	L0	
Catégorie	N/A	APPL	APPL	op.pl.5	Composants certifiés	NON			NON APPLICABLE PUISQU'IL S'AGIT D'UNE MESURE POUR LES SYSTÈMES DE CATÉGORIE MOYENNE ET ÉLEVÉE

Figure 2. Extrait d'une éventuelle Déclaration d'Applicabilité

L'extrait de la grille ci-dessus, qui représente un système à catégorie BASIQUE, nous permet d'observer la manière de décrire l'applicabilité concrète des mesures [org.1] et [org.2]. Dans la colonne "Niveau d'implémentation", G0 signifie que la mesure n'est pas implémentée, G1 que cette implémentation est en cours et G2 que la mesure est implémentée.

6.2. Décalogue de recommandations générales

Vous trouverez ci-dessous un décalogue de recommandations à prendre en compte pour rédiger une Déclaration d'Applicabilité dans le cadre de l'ENS.

DÉCALOGUE DE RECOMMANDATIONS POUR LA DÉCLARATION D'APPLICABILITÉ (ENS)	
1	Tout d'abord, il convient d'évaluer les actifs essentiels (de type "information" et "service").
2	Pour évaluer les actifs, il faut fixer un niveau de sécurité pour chacune des dimensions : confidentialité [C], intégrité [I], disponibilité [D], authenticité [A] et traçabilité [T]. Ce niveau est fixé en fonction de l'impact d'un incident de sécurité sur l'une des dimensions.
3	Si l'actif essentiel est de type "service", il est recommandé d'évaluer d'abord la dimension "disponibilité" [D], car les exigences en matière de confidentialité, d'intégrité, d'authenticité et de traçabilité sont généralement une instanciation des actifs de type "information".
4	Établir la catégorie du système (BASIQUE, MOYENNE ou ÉLEVÉE) en fonction des niveaux de sécurité attribués aux différentes dimensions, en tenant compte du fait que l'attribution d'une catégorie au système nécessite la définition du niveau d'implémentation des mesures à appliquer et que la catégorie du système correspondra au niveau de sécurité le plus élevé parmi ceux qui ont été attribués.
5	Sélectionnez les mesures qui s'appliquent au système en fonction de leur catégorie, sur un total de 45 mesures.
6	Sélectionnez les mesures qui s'appliquent au système en fonction de leur niveau de sécurité, sur un total de 28 mesures.

7	Utilisez le simulateur développé par le CCN-CERT, qui permet de déterminer automatiquement la Déclaration d'Applicabilité, en saisissant les niveaux de sécurité pour toutes les dimensions de l'actif.
8	Indiquez en détail la correspondance entre les mesures compensatoires qui ont déjà été mises en œuvre et les mesures compensatoires énumérées dans l'Annexe II; de même pour toute mesure de surveillance supplémentaire. Cet ensemble sera formellement approuvé par le responsable de sécurité.
9	S'il existe des mesures compensatoires dans la Déclaration d'Applicabilité, détaillez les paramètres suivants pour chacune d'entre elles : champ d'application, limitations ou restrictions, objectif, risque identifié, définition de la mesure compensatoire, validation de la mesure compensatoire et maintenance. Le contenu de ces paramètres est précisé dans le guide CCN-STIC-819 "Mesures compensatoires".
10	Pour la rédaction de la Déclaration d'Applicabilité, utilisez un document rédigé par vous-même ou le modèle officiel fourni par le CCN-CERT, en tenant compte des profils de conformité validés par le CCN dans les guides CCN-STIC respectifs.

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es